Deepak Maram

Cornell Tech, 2 West Loop Rd, NYC - 10044
sm2686@cornell.edu
https://sites.google.com/view/deepak-maram/home

Research

I am broadly interested in computer security, privacy, and applied cryptography. My recent focus has largely been around decentralized systems like blockchains. My research has led to direct industry adoption. CHURP [CCS19] is on Oasis Labs product road map. DECO [CCS20] is licensed from Cornell by Chainlink.

Education

2018 - present **Ph.D. Candidate in Computer Science**.
Cornell University, USA
Advisor: *Ari Juels*, GPA: 3.71/4

2012 - 16 **B.Tech in Computer Science with Honors**.
Indian Institute of Technology, Bombay, India
GPA: 8.91/10

Industry Experience

June 2020–Oct 2020 **Cryptography Research Engineer Internship**, *Cloudflare*, Remote.
Devised a privacy-preserving, usable alternative to CAPTCHA using WebAuthn (Web Authentication) as the base layer and a novel cryptographic scheme as an anonymity layer. The scheme involved zero knowledge protocols and accumulators. Implemented for web in JavaScript.

July 2016–Dec 2017 **Member of Technical Staff**, *Oracle*, Bangalore.
Back-end Java Developer for the GlassFish application server. Implemented several core features, bug fixes in the deployment module that released in Java EE RI 8. Handled the external transfer of several important artifacts of GlassFish project such as Github issues, bug reports using Bash and NodeJS scripting.

Honors / Awards

2018 Awarded University Fellowship by Cornell University
2012 Secured All India Rank 12 in *IIT-JEE* out of 500,000 students
2012 Secured All India Rank 36 in *AIEEE* out of 11,00,000 students
2012 Recipient of KVPY scholarship and attended VIJYOSHI Camp
2011 Awarded merit certificate for being in top 1% in National Standard Examination - Astronomy

Technical Skills

Languages C++ (4000 lines), Python (3000 lines), Java (3000 lines), JavaScript (1000 lines), Rust (500 lines)

Selected Projects

2020 **CanDID: A platform for Decentralized Identity (DID)**, *Cornell*.
Developed a privacy-preserving decentralized identity system whose key features include legacy compatibility (ports existing credentials like users' SSN), key management (provides easy-to-use key recovery), Sybil-resistance (ensures one token per user) and accountability (bars sanctioned users for compliance).

2019 **DECO: Liberating Web Data Using Decentralized Oracles**, *Cornell*.
Designed a novel privacy-preserving oracle protocol that makes internet data accessible to smart contracts. Implemented a zero-knowledge parser to process HTTPS session transcripts in JSON and HTML formats. Built the parser in xjsnark, a Java-like language that outputs zkSNARK (libsnark) circuits.

2019 **CHURP: Dynamic-committee Proactive Secret Sharing**, *Cornell*.
Devised a novel cryptographic protocol to facilitate dynamic committees in secret sharing, thus enabling a decentralized key management system. Improved the state-of-the-art protocol to incur atleast 1000x less communication cost for large committees.

2018 **SkinnerDB: Regret-Bounded Query Evaluation via Reinforcement Learning**, *Cornell*.
Expanded the query processing engine of a novel learning-based DBMS (SkinnerDB) by supporting multiple new query types. Involved understanding and implementing query optimization strategies in Java. Demonstrated orders of magnitude improvement over a traditional DBMS for some difficult-to-optimize queries.

2016 **New Internet Architectures: SCION**, *ETH Zurich*.
Research Internship, *Guide: Adrian Perrig*
Built a discrete event simulator and topology generator for a novel internet architecture (SCION) in Python in order to perform large-scale network simulations. Devised a new category of attack in SCION that exploits the network architecture to gain extended access to favorable routing paths, and subsequently proposed defenses that render such an attack impractical.

2015 **Bit-rate adaptation in wireless networks**, *IIT Bombay*.
R&D Project, *Guide: Mythili Vutkuru*
Experimented with lookaround rate of a popular wireless bit-rate adaptation algorithm (Minstrel) using a network simulator, ns3. Formulated bit-rate adaptation as an instance of the Multi-armed bandit problem.

2015 **Building a compiler from scratch**, *IIT Bombay*.
Course Project, *Guide: Prof. Amitabha Sanyal*
Developed a lexical analyzer using flex and a parser using bison, as part of implementing a compiler for a C-style language. Using Sethi-Ullman algorithm, we performed register allocation efficiently.

Posters / Talks

2020 **CanDID: A Decentralized Identity System**.
Presented our work at the Hyperledger Identity Working Group.
Presented our work at the 31st Internet Identity Workshop.
Presented our work at the Travel Rule Information Sharing Architecture Governance Call.

2019 **CHURP: Dynamic-committee Proactive Secret Sharing**.
Presented our work at the ACM conference on Computer and Communication Security (CCS), London.
Gave a talk at the Initiative for Cryptocurrencies and Contracts (IC3) Winter Retreat, Interlaken.

2018 **SkinnerDB: Regret-Bounded Query Evaluation via Reinforcement Learning**.
Presented a poster at the Conference on Very Large Data Bases (VLDB) 2018, Rio.

Graduate Course Work

Advanced Programming Languages, Advanced Operating Systems, Intro to Computer Vision, Security & Privacy Technologies, Cryptocurrency and Smart Contracts, Advances in Intelligent and Learning Agents (UG), Advanced Cryptography (UG), Computational Ring Theory (UG), Graph Theory (UG)

Publications

[SP21] **CanDID: Can-Do Decentralized Identity with Legacy Compatibility, Sybil-Resistance, and Accountability**.
D. Maram, H. Malvai, F. Zhang, N. Jean-Louis, A. Frolov, T. Kell, T. Lobban, C. Moy, A. Juels, and A. Miller. *In IEEE S&P 2021. To appear.*

[CCS20] **DECO: Liberating Web Data Using Decentralized Oracles**, *deco.works*.
F. Zhang, **D. Maram**, H. Malvai, S. Goldfeder, and A. Juels. *In Proceedings of the 2020 ACM Conference on Computer and Communications Security (CCS).*

[CCS19] **CHURP: Dynamic-committee Proactive Secret Sharing**, *churp.io*.
D. Maram, F. Zhang, L. Wang, A. Low, Y. Zhang, A. Juels, and D. Song. *In Proceedings of the 2019 ACM Conference on Computer and Communications Security (CCS).*

[SIGMOD19] **SkinnerDB: Regret-Bounded Query Evaluation via Reinforcement Learning**.
I. Trummer, S. Moseley, **D. Maram**, S. Jo, and A. Antonakakis. *In Proceedings of the 2019 International Conference on Management of Data (SIGMOD).*

Service / Extra-curriculars

2019 - 20 Served as the treasurer of PhD student organization At Cornell Tech (PACT)

2014 Awared first prize at the *XLR8* competition for designing a Wireless Controlled Bot

2003 - 07 Won first prize in several district-level chess competitions and participated in state-level competitions